4 Jurisdictie en grensoverschrijdende digitale opsporing

Jan-Jaap Oerlemans[1]

4.1 Inleiding

Cybercriminaliteit is grensoverschrijdend. Zowel de verdachten als het bewijs bevinden zich vaak buiten de territoriale grenzen van het land van waaruit de opsporing plaatsvindt. Cybercriminaliteit en de opsporing daarvan krijgen daardoor al snel een internationale dimensie. Hoewel praktisch gezien voor internetgebruikers de territoriale grenzen van een staat op internet geen rol van betekenis hebben, zijn territoriale grenzen juridisch gezien nog steeds heel belangrijk. Binnen hun eigen territorium bepalen staten namelijk op welke manier zij gedragingen strafbaar stellen, onder welke voorwaarden opsporingsinstanties hun bevoegdheden mogen inzetten en onder welke regels personen worden berecht. Met andere woorden, terwijl internet 'deterritorialisering' met zich mee brengt, blijven staten tegelijkertijd vasthouden aan principes in het internationaal recht die grotendeels op een territoriale leest zijn geschoeid. In dit hoofdstuk worden de belangrijkste aspecten van jurisdictie behandeld en wordt verkend in hoeverre opsporingshandelingen in een online context grensoverschrijdend mogen plaatsvinden.

Het uitgangspunt is in dit hoofdstuk dat er geen bijzonder regime voor jurisdictie in een online context geldt. 'Cyberspace' wordt ook wel gezien als een 'virtuele omgeving' waarbinnen personen en overheidsautoriteiten opereren. Internetgebruikers ervaren internet ook vaak als een omgeving waarbinnen andere regels gelden. Sommige auteurs zijn van mening dat een ander juridisch regime op internet zou moeten gelden, vergelijkbaar met de vrijheid van de volle zee (*mare liberum*), waarbij alle staten het recht hebben om in vrijheid hun recht toe te passen en uit te voeren, behoudens afspraken die zijn gemaakt met andere staten die hun gedrag beperken.[2] Binnen het internationale recht wordt echter *niet* de lijn gevolgd dat andere regels (zouden moeten) gel-

1 Mr. dr. J.J. Oerlemans is als onderzoeker verbonden aan eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden. Dit hoofdstuk bouwt deels voort op het werk van prof. mr. H.W.K. Kaspersen, 'Het Cybercrime-verdrag van de Raad van Europa', zoals verschenen in de tweede druk van dit boek in 2007.

2 Zie bijvoorbeeld Hildebrandt 2013 en het overzicht van theorieën in Koops & Goodwin 2014.

den voor gedragingen die via computers en internet plaatsvinden.[3] Daarom worden in dit hoofdstuk de huidige principes en beginselen van het internationale recht toegepast in de context van cybercriminaliteit.
Het hoofdstuk begint met een inleiding met betrekking tot de begrippen 'jurisdictie' en 'rechtshulp'. Daarbij wordt uitgelegd op welke manier deze begrippen zich verhouden tot opsporingsonderzoeken naar cybercriminaliteit. Vervolgens wordt kort het Cybercrimeverdrag besproken, als belangrijk ankerpunt voor de internationale samenwerking bij digitale opsporing. Daarna wordt aandacht besteed aan de actuele problematiek omtrent het grensoverschrijdend uitvoeren van digitale opsporingshandelingen door opsporingsinstanties in strafrechtelijke onderzoeken. Het hoofdstuk sluit af met een overzicht van lopende initiatieven om te komen tot een toekomstige regeling van unilaterale grensoverschrijdende opsporing.

4.2 Jurisdictie en rechtshulp

Jurisdictie is de rechtsmacht van een staat of een ander regelgevend orgaan om wetten te maken, toe te passen en uit te voeren met betrekking tot het gedrag van personen, binnen de grenzen van het internationale recht.[4] Binnen het strafrecht onderscheiden we daarbij wetgevende jurisdictie en uitvoerende jurisdictie.[5]
Deze twee jurisdictiebegrippen worden in deze paragraaf verder uitgewerkt, binnen de context van cybercriminaliteit. Daarnaast wordt kort het instrument van de kleine rechtshulp toegelicht, dat veelal moet worden ingezet bij de grensoverschrijdende bewijsgaring door opsporingsautoriteiten.

4.2.1 *Wetgevende jurisdictie*

Opsporingsautoriteiten in een staat mogen slechts een opsporingsonderzoek starten als zij wetgevende jurisdictie hebben, ook wel 'rechtsmacht' genoemd. De wetgevende jurisdictie wordt in de eerste plaats bepaald door het territorialiteitsbeginsel. Dit beginsel houdt in dat een staat rechtsmacht kan aannemen over een element van een strafgedraging binnen het territorium van die staat.[6] Het begrip 'jurisdictie' is sterk verbonden met het begrip 'soevereiniteit'. Binnen het internationale recht wil de soevereiniteit van staten zeggen dat staten hun eigen wet- en regelgeving kunnen toepassen

3 Zie ook, onder andere, Koops & Goodwin 2014 en Tallinn Manual 2017, p. 51. Kaspersen gaf in zijn versie van dit hoofdstuk in 2007 aan dat de ontwerpers van het verdrag niet de gedachte deelden dat internationale communicatienetwerken zouden noodzaken tot de ontwikkeling van nieuwe rechtsmachtconcepten.
4 Zie, onder andere, Mann 1964, p. 1, Mann 1984, p. 9 e.v., Lowe 2006, p. 335, Shaw 2008, p. 469 en Tallinn Manual 2017, p. 51.
5 Met deze onderverdeling wordt aangesloten bij onder andere Mann 1964, p. 1, Akehurst 1974, p. 179, Mann 1984, p. 9, O'Keefe 2004, p. 737-738 en Kohl 2007, p. 16. Adjudicatieve jurisdictie, kort gezegd de rechtsmacht van rechtbanken om te oordelen over feiten, wordt hier als onderdeel van de wetgevende macht gezien.
6 Zie uitgebreid Blakesley 2008, p. 93.

op personen en objecten binnen hun territorium en op gedragingen die plaatsvinden binnen hun territorium.[7]
De plek waar de strafbare gedraging is gepleegd wordt *locus delicti* genoemd.[8] In de *Lotus*-zaak in 1927 heeft het Permanent Hof van Internationale Justitie (nu het Internationaal Gerechtshof genoemd) bevestigd dat staten ook onder omstandigheden jurisdictie kunnen uitoefenen over strafbare gedragingen die in het buitenland worden gepleegd.[9] Zo oefent Nederland wetgevende rechtsmacht uit over bepaalde in het buitenland gepleegde strafbare feiten (zie artikel 4 e.v. Sr). Op grond van artikel 539a e.v. Sv kunnen Nederlandse opsporingsinstanties ook overgaan tot opsporing van elders gepleegde strafbare feiten, echter alleen voor zover dat in overeenstemming is met het internationale recht (zie paragraaf 4.2.2).

Territorialiteitsbeginsel en de effectendoctrine
Het territorialiteitsbeginsel is het primaire beginsel op basis waarvan staten jurisdictie aannemen.[10] Ook in het Cybercrimeverdrag is expliciet gemaakt dat het territorialiteitsbeginsel kan worden toegepast voor het aannemen van rechtsmacht.[11] De toepassing van dit principe in een online context wordt door de experts van het gezaghebbende Tallinn Manual helder uitgelegd. Staten mogen jurisdictie uitoefenen over:
1. de IT-infrastructuur en de gedragingen van personen via computers en internet binnen hun territorium;
2. de activiteiten die door computers en netwerken binnen hun territorium worden gefaciliteerd[12]; of
3. de activiteiten die door computers en netwerken worden gefaciliteerd en een "substantieel effect" creëren binnen hun territorium.[13]

In cybercrimezaken kunnen staten op basis van het territorialiteitsbeginsel in veel gevallen eenvoudig jurisdictie aannemen.[14] Uiteraard is dat, zoals hierboven is aangegeven, mogelijk als personen op hun eigen territorium via computers en netwerken strafbare gedragingen plegen. Ook als van een computer gebruik wordt gemaakt bij het plegen van een computermisdrijf binnen het territorium van een staat, kan op grond van het territorialiteitsbeginsel jurisdictie worden aangenomen. Staten kunnen op ba-

7 Zie ook Tallinn Manual 2017, p. 52.
8 Zie uitgebreid over de locus delicti in de context van cybercrime: Van Wijk 1989 en Wolswijk 1998.
9 Zie PCIJ, SS Lotus (*Frankrijk t. Turkije*) 1927, PCIJ Reports, Series A, No. 10, p. 19: "Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable".
10 Zie Akehurst 1974, p. 152 en meer recent hierover onder andere Ryngaert 2009.
11 Artikel 22 lid 1 sub a Cybercrimeverdrag.
12 Deze activiteiten worden 'cyberactiviteiten' genoemd in het Tallinn Manual 2017.
13 Tallinn Manual 2017, p. 52.
14 In Nederland is dit duidelijk gemaakt in artikel 2 Sv: "De Nederlandse strafwet is toepasselijk op ieder die zich in Nederland aan enig strafbaar feit schuldig maakt".

sis van het territorialiteitsbeginsel rechtsmacht toepassen over alle gegevens en computers die zich op hun territorium bevinden.[15]
Echter, hoe verder het gebruik van de computer afstaat van de gevolgen die worden veroorzaakt in het territorium van een staat, hoe minder het voor de hand ligt om rechtsmacht aan te nemen.[16] In het Tallinn Manual 2.0 wordt bijvoorbeeld opgemerkt dat de experts het niet met elkaar eens zijn met betrekking tot de vraag of "stromende gegevens binnen de IT-infrastructuur van een staat" voldoende grond opleveren om jurisdictie aan te nemen.[17] Op grond van de zogenoemde 'effectendoctrine' kan dan mogelijk jurisdictie worden aangenomen. Dit beginsel houdt in deze context in dat de schadelijke gedragingen hun oorsprong vinden buiten het territorium van een staat, maar bepaalde effecten hebben binnen het territorium van een staat. Het is internationaalrechtelijk geaccepteerd dat jurisdictie wordt aangenomen op basis van de effectendoctrine, voor zover er een 'substantiële verbinding' bestaat tussen het delict en het territorium van de staat.[18]
De kritiek op toepassing van de effectendoctrine door staten is dat het wel érg eenvoudig wordt het strafrecht van de ene staat toe te passen op gedragingen van een persoon die zich mogelijk in een andere staat bevindt. Deze persoon kent mogelijk de wetten van een andere staat niet. Het bedreigt, met andere woorden, de rechtszekerheid van de betrokkene. Landsgrenzen van staten hebben van oudsher een 'kenbaarheidsfunctie'. Het kenbaarheidsprincipe houdt in dat de toepassing van een strafwet kenbaar of voorzienbaar moet zijn voor de persoon die eraan wordt onderworpen. Van der Net pleit ervoor voorzichtig om te gaan met het aannemen van jurisdictie en bij voorkeur een beperkter territorialiteitsbeginsel aan te nemen bij computercriminaliteit.[19] Het idee is dat steeds een zinvolle relatie moet bestaan tussen het feitencomplex en de staat die daarop zijn strafwet wil toepassen. Ook de experts van het Tallinn Manual 2.0 waarschuwen dat staten zorgvuldig moeten zijn bij het toepassen van wetgevende jurisdictie bij handelingen die hun oorsprong hebben in het buitenland: dit is slechts toegestaan als er "substantiële effecten" op het territorium van de betrokken staat optreden.[20]

Personaliteitsbeginsel
Het Cybercrimeverdrag geeft daarnaast ook aan dat op grond van het "actief personaliteitsbeginsel" rechtsmacht kan worden aangenomen.[21] Het actief personaliteitsbeginsel houdt in dat staten wetgevende jurisdictie mogen aannemen als de dader van het

15 Zie ook Tallinn Manual 2017, p. 63.
16 Zie in soortgelijke bewoordingen ook Tallinn Manual 2017, p. 58: "'The International Group of Experts agreed that the more attenuated the casual relationship between the cyber operations and the effects they cause in a state, the less compelling the case for applying the effects doctrine".
17 Tallinn Manual 2017, p. 52.
18 Tallinn Manual 2017, p. 57.
19 Zie Van der Net 2000, p. 380 e.v..
20 Tallinn Manual 2017, p. 61.
21 Artikel 22 lid 1 sub d Cybercrimeverdrag. Zie ook artikel 7 Sr en artikel 3 lid 2 van het Besluit internationale verplichtingen extraterritoriale rechtsmacht.

delict de nationaliteit van de staat heeft die het onderzoek start. In het Cybercrimeverdrag is het daarbij een nadere voorwaarde dat het feit tevens strafbaar is onder het recht ter plaatse – het vereiste van "dubbele strafbaarheid". Deze voorwaarde vervalt indien het territoir tot de rechtsmacht van geen enkele staat behoort.

Beschermingsbeginsel
Het is ten slotte denkbaar dat het 'beschermingsprincipe' van toepassing is bij het aannemen van jurisdictie in de context van cybercriminaliteit. In het Tallinn Manual 2.0 wordt aangegeven dat het beginsel van toepassing kan zijn indien cybercriminaliteit zeer grote gevolgen met zich kan meebrengen. Dat kan het geval zijn als het delict (a) mensenlevens in gevaar brengt; (b) de nationale veiligheid of sleutelfuncties van de staat in gevaar brengt; of (c) als cyberterrorisme maatschappelijke ontwrichting met zich meebrengt.[22] Het beginsel onderscheidt zich van de effectendoctrine bij het territorialiteitsbeginsel, omdat het beschermingsbeginsel beperkt is tot een kleinere categorie van delicten die niet noodzakelijk enige effecten veroorzaken binnen het territorium van een staat.[23]

Positieve jurisdictieconflicten
Het hierboven besproken territorialiteitsprincipe, actief personaliteitsbeginsel en beschermingsprincipe om jurisdictie aan te nemen, maken duidelijk dat bij cybercriminaliteit meerdere staten tegelijk eenvoudig jurisdictie kunnen aannemen.[24] Het feit dat veel staten potentieel jurisdictie kunnen aannemen en een onderzoek starten brengt met zich mee dat 'positieve jurisdictieconflicten' kunnen ontstaan.[25] Meerdere staten nemen dan tegelijk rechtsmacht aan en dat kan leiden tot conflicten over wie voorrang heeft bewijs te verzamelen en de verdachte te berechten. In het Cybercrimeverdrag is een bepaling opgenomen (artikel 22 lid 5) die verdragsstaten verplicht stelt met elkaar in overleg te gaan om positieve jurisdictieconflicten op te lossen. In de praktijk vindt overigens ook bij Europol en Eurojust afstemming plaats met betrekking tot internationale opsporingsonderzoeken naar cybercriminaliteit. Europol heeft een eigen 'E3 European Cybercrime Centre', gevestigd in Den Haag.

4.2.2 *Uitvoerende jurisdictie*

Uitvoerende of executieve jurisdictie omvat de macht van een staat om nakoming van wetten te verzekeren door op een of andere wijze zijn macht uit te oefenen. De bewijsgaringsactiviteiten van opsporingsinstanties vallen onder de uitvoerende jurisdictie van een staat. Kenmerkend voor deze vorm van jurisdictie is dat – in tegenstelling tot de wetgevende jurisdictie – de uitvoerende jurisdictie territoriaal strikt beperkt is. Dat wil zeggen dat de uitvoerende jurisdictie niet verder reikt dan het territorium van de

22 Tallinn Manual 2017, p. 64.
23 Tallinn Manual 2017, p. 64.
24 Zie ook Herrera-Flanigan 2006, p. 314-316 en Klip & Massa 2010, p. 116.
25 Zie ook uitgebreid over positieve jurisdictieconflicten: Brenner 2006.

staat. In de eerder aangehaalde *Lotus*-zaak wordt de territoriale beperking van de uitvoerende jurisdictie tot de grenzen van een staat uitgewerkt.[26] Kort gezegd mogen staten geen opsporingsonderzoek in het buitenland uitvoeren, zonder ad-hoc toestemming van de betrokken staat of een verdragsrechtelijke basis.[27]
De primaire reden waarom opsporingsactiviteiten niet zonder toestemming of verdragsbasis in het buitenland mogen plaatsvinden, is dat de bewijsgaring een exclusieve taak van een staat is, waarbij de staat de opsporing op zijn eigen manier regelt.[28] Een inmenging van de opsporingsautoriteiten van een andere staat in die exclusieve overheidstaak – zonder toestemming of verdragsbasis – brengt een soevereiniteitsschending voor de betrokken staat met zich mee.
Toepassing van het territorialiteitsprincipe in het internationale strafrecht en de territoriale beperking van de uitvoeringsrechtsmacht betekent ook dat vaak *lokale* wetgeving de strafbare gedragingen omschrijft, *lokale* opsporingsautoriteiten aan bewijsgaring doen onder hun eigen regelgeving en de *lokale* instanties mensen vervolgen voor cybercriminaliteit in hun eigen rechtbanken. De opsporing en vervolging van cybercriminaliteit blijft hierdoor in grote mate een lokale aangelegenheid, terwijl deze criminaliteit bij uitstek een *grensoverschrijdend* karakter heeft, aangezien de techniek achter internet geen territoriale grenzen kent.[29] Door gebruikmaking van rechtshulp kunnen staten wel op formele wijze bewijs verzamelen of uitleveringsverzoeken doen in het kader van opsporingsonderzoeken.

4.2.3 *De kleine rechtshulp en rechtshulpverdragen*

De 'kleine rechtshulp'[30] is de formele procedure waarbij staten andere staten verzoeken bewijs te verzamelen op buitenlands grondgebied.[31] Staten kunnen bovendien in verdragen overeenkomen onder welke voorwaarden eenzijdige grensoverschrijdende bewijsgaringsactiviteiten mogen plaatsvinden. Nederland kent veel bilaterale en multilaterale verdragen waarin bepaalde grensoverschrijdende bewijsgaringsactiviteiten geregeld worden. Binnen de Europese Unie zijn bijvoorbeeld het EU-rechtshulpver-

26 Zie PCIJ, SS Lotus (*Frankrijk t. Turkije*), 1927, *PCIJ Reports*, Series A, nr. 10, p. 18-19: "The first and foremost restriction imposed by international law upon a State is that – failing existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention".

27 Zie Mann 1964, p. 44-49, Akehurst 1974, p. 145 en Reijntjes, Mos & Sjöcrona 2008, p. 257. Zie ook Tallinn Manual 2017, p. 66: "*Rule 11 – Extraterritorial jurisdiction.* A State may only exercise extraterritorial enforcement jurisdiction in relation to person, objects, and cyber activities on the basis of: (a) a specific allocation of authority under international law; or (b) valid consent by a foreign government to exercise jurisdiction on its territory".

28 In het Tallinn Manual 2.0 (2017, p. 21) wordt dit een cyberoperatie genoemd die "interferes with the inherently governmental functions of a State". In de praktijk is de vrijheid van staten om hun eigen regels te maken en overheidsmacht toe te passen vaak beperkt door internationale (mensenrechten)verdragen.

29 J.J. Oerlemans 2017a, p. 58.

30 Grote rechtshulp is de overname van een strafprocedure of de tenuitvoerlegging van een buitenlands vonnis. Dit hoofdstuk gaat alleen in op de kleine rechtshulp.

31 Reijntjes, Mos & Sjöcrona 2008, p. 263.

drag, het rechtshulpverdrag tussen lidstaten en het Europees onderzoeksbevel in het bijzonder van belang, ook in opsporingsonderzoeken naar cybercriminaliteit.[32] Ook het Cybercrimeverdrag bevat de nodige bepalingen omtrent de rechtshulp.[33] Van bijzondere betekenis is ook artikel 26 Cybercrimeverdrag, dat verdragsstaten een wettelijke basis biedt uit eigen beweging informatie te verstrekken aan de opsporingsdiensten van een andere staat die is verkregen in het kader van een strafrechtelijk onderzoek. Het valt buiten het bestek van dit hoofdstuk de specifieke relevante bepalingen van deze verdragen voor het vergaren van bewijs op buitenlands territorium in cybercrimezaken in detail te behandelen. Als voorbeeld wordt in de volgende paragraaf kort ingegaan op de rol van het Cybercrimeverdrag bij de internationale samenwerking in strafzaken met een digitale component, omdat dit verdrag wereldwijd een centrale rol vervult in de onderlinge afstemming van wetgeving en procedures.

4.3 Het Cybercrimeverdrag en internationale samenwerking in digitale opsporing[34]

4.3.1 *Geschiedenis en internationale reikwijdte*

Het Cybercrimeverdrag kent een lange voorgeschiedenis. De huidige tekst van het verdrag vindt zijn oorsprong in twee aanbevelingen van de Raad van Europa met betrekking tot de bestrijding van computercriminaliteit.[35] Met de aanbevelingen werd echter niet het gewenste niveau van harmonisatie van wetgeving bereikt. Daarom werd besloten te streven naar een bindende overeenkomst in de vorm van een verdrag. De opdracht van de Raad van Europa was te onderzoeken in hoeverre aanvullende bepalingen van materieel strafrecht internationale samenwerking kunnen bevorderen. Op het gebied van het formele strafrecht diende onderzocht te worden in hoeverre er in het licht van de aanbeveling van 1995 behoefte was aan specifieke opsporingsbevoegdheden. Met name ging het daarbij om de grensoverschrijdende netwerkzoeking, het onderzoek en het veiligstellen van informatie in computersystemen en op websites, het ontoegankelijk maken van inbreukmakend elektronisch materiaal en het vorderen van medewerking van personen, bijvoorbeeld met betrekking tot kennisname van versleutelde informatie. Ook bevatten de 'terms of reference' de opdracht een oplossing te

32 Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken, 20 april 1959, Straatsburg, *Trb.* 1965, 10, Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, 29 mei 2000, *Trb.* 2000, 96 en Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken, *OJ* L 130/1, geïmplementeerd op 17 mei 2017, *Stb.* 2017, 231.

33 Artikel 23-34 van het Cybercrimeverdrag.

34 Voor een uitgebreider overzicht, zie Kaspersen 2007.

35 Zie Recommendation R (89) 9, 'Computer-related Crime', van 13 september 1989 en Recommendation R (1995) 13, 'Problems of criminal procedural law connected with information technology' van 11 september 1995.

geven voor positieve en negatieve rechtsmachtconflicten in verband met delicten begaan in cyberspace.[36]
Het Cybercrimeverdrag heeft veel van de doelstellingen uiteindelijk bereikt, alhoewel bepaalde onderwerpen te gevoelig bleken te liggen voor de verdragsstaten. Het gehele proces van ontwerp tot openstelling voor ondertekening van het Verdrag nam bijna zes jaar in beslag. Op 8 november 2001 is het verdrag door het Comité van Ministers te Straatsburg aanvaard en op 23 november 2001 te Boedapest door dertig staten ondertekend, waaronder Nederland.[37] Nederland heeft het verdrag op 16 november 2006 geratificeerd en op 1 maart 2007 is het verdrag voor Nederland in werking getreden.[38]
Het Cybercrimeverdrag wordt door velen als het belangrijkste verdrag voor cybercrime-onderzoeken gezien. Kaspersen verhaalt in zijn uitgebreide bespreking van het verdrag hoe het "in een afzonderlijke vergadering in het prachtige Parlementsgebouw van Boedapest door maar liefst dertig staten werd ondertekend: een unicum in de geschiedenis van de Raad van Europa".[39] Nog elk jaar ondertekenen en ratificeren nieuwe staten het Cybercrimeverdrag. Inmiddels hebben vrijwel alle lidstaten van de Raad van Europa het verdrag geratificeerd; de enige uitzonderingen zijn Ierland, de Russische Federatie (de enige lidstaat die het verdrag niet heeft ondertekend), San Marino en Zweden.
Een grote meerwaarde van het Cybercrimeverdrag van de Raad van Europa ten opzichte van andere regionale verdragen is dat op grond van artikel 37 van het verdrag ook staten kunnen toetreden die *geen* lid zijn van de Raad van Europa. Staten hebben dat ook op grote schaal gedaan. Het verdrag is inmiddels geratificeerd door de navolgende niet-lidstaten: Argentinië, Australië, Canada (*), Chili, Costa Rica, Dominicaanse Republiek, Filipijnen, Israël, Japan (*), Kaapverdië, Marokko, Mauritius, Panama, Paraguay, Senegal, Sri Lanka, Tonga en de Verenigde Staten (*). De met een * gemarkeerde landen namen deel aan de voorbereidingen van het verdrag (juist met het oog op een meer mondiale uitwerking van het verdrag) en ondertekenden het verdrag op 23 november 2001. Zuid-Afrika nam eveneens deel aan de voorbereidingen en ondertekende het verdrag, maar heeft het (nog) niet geratificeerd. Per 1 augustus 2018 hebben in totaal 61 staten het verdrag geratificeerd.[40]

4.3.2 *Belang van het verdrag voor internationale samenwerking*

Het Cybercrimeverdrag is om drie redenen belangrijk voor cybercrime-onderzoeken in een internationale context.[41] Ten eerste harmoniseert het verdrag belangrijke straf-

36 Kaspersen 2007, p. 140-141.
37 Officiële titel: 'Convention on Cyber Crime', ETS 185. In het Nederlands: 'Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken', *Trb.* 2002, 18. Het Cybercrimeverdrag wordt naar de plaats van handeling ook wel het 'Verdrag van Boedapest' genoemd.
38 *Trb.* 2007, 10.
39 Kaspersen 2007, p. 138.
40 Een overzicht van ondertekeningen en ratificaties is te vinden op https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (laatst geraadpleegde 1 augustus 2018).
41 Zie ook Oerlemans 2017a, p. 58-59.

baarstellingen, zoals computervredebreuk, *denial-of-service*-aanvallen, het bezitten, vervaardigen en verspreiden van kwaadaardige software, computergerelateerde valsheid en fraude en (virtuele) kinderpornografie (zie artikel 2-13 Cybercrimeverdrag). Door deze harmonisatie wordt bevorderd dat aan het vereiste van dubbele strafbaarheid is voldaan, wat een belangrijk vereiste is voor het verlenen van internationale rechtshulp.
Ten tweede verplicht het verdrag tot het implementeren van opsporingsbevoegdheden in nationale wetgeving met betrekking tot het vorderen en veiligstellen van gegevens. Gezien het belang van bijvoorbeeld de mogelijkheid een IP-adres te traceren en vervolgens gebruikersgegevens en verkeersgegevens te vorderen bij online service providers, is het noodzakelijk dat staten in deze mogelijkheid in hun nationale wetgeving voorzien, evenals de mogelijkheid om laagdrempelig gegevens te bevriezen in afwachting van de voor rechtshulp vereiste formele papieren. Het Cybercrimeverdrag heeft dit in de bepalingen met betrekking tot het formeel strafrecht bewerkstelligd (zie artikel 14-21 Cybercrimeverdrag). Deze harmonisatie bevordert dat lidstaten voldoende digitale opsporingsbevoegdheden beschikbaar hebben, zodat zij op verzoek van andere lidstaten digitaal bewijs op hun grondgebied kunnen vergaren.
Ten derde draagt het verdrag bij aan de mogelijkheid tot snelle bewijsgaring met behulp van rechtshulp. Naast uitlevering (artikel 24) bevat het verdrag een uitgebreide afdeling over wederzijdse rechtshulp (artikel 25 en 27-35). Deze bepalingen verzekeren dat lidstaten elkaar rechtshulp verlenen, ook als zij geen onderling (bi- of multilateraal) rechtshulpverdrag kennen. De titel over wederzijdse rechtsbijstand bevat onder andere bepalingen over urgente bevriezing van computergegevens (artikel 29) en spoedige verstrekking van die verkeersgegevens die nodig zijn om een andere staat om rechtshulp te verzoeken (artikel 30), alsmede het verlenen van bijstand door op verzoek van een andere staat opgeslagen computergegevens veilig te stellen, bijvoorbeeld via doorzoeking (artikel 31), real-time verkeersgegevens te vergaren (artikel 33) en de inhoud van communicatie te onderscheppen (artikel 34).
Een belangrijke faciliterende procedure voor het verlenen van rechtshulp is geregeld in artikel 35. Het verdrag schrijft hier voor dat elke verdragsstaat een contactpunt creëert voor rechtshulpverzoeken in cybercrimezaken dat 24 uur per dag, zeven dagen in de week beschikbaar moet zijn. Bovendien kunnen rechtshulpverzoeken naar instanties worden gestuurd die de verzoeken met betrekking tot cybercriminaliteit of digitale opsporing centraal behandelen en de rechtshulpverzoeken coördineren. Het is aan het nationale recht overgelaten welke bevoegdheden precies aan het contactpunt voor cybercriminaliteit worden toegekend. De verdragstekst doet een aantal suggesties, zoals het geven van technisch advies, het verstrekken van informatie over het nationale recht, het uitvoeren van de voorlopige maatregelen van de artikelen 29 en 30, het lokaliseren van verdachten en het vergaren van bewijs. Lid 3 van artikel 35 bevat een zorgplicht voor lidstaten om voldoende getraind en toegerust personeel beschikbaar te houden. Het bleek daarbij een brug te ver ook resultaatsverplichtingen op te nemen, door bijvoorbeeld verplicht te stellen binnen een bepaalde tijd antwoord te geven of het verzoek uit te voeren. In de EU-richtlijn aanvallen op informatiesystemen is wel

een bepaling opgenomen dat de verzochte instantie binnen acht uur moet reageren op een rechtshulpverzoek.[42]

In andere regio's in de wereld zijn ook verdragen omtrent cybercriminaliteit opgesteld. Deze verdragen zijn vaak beperkt tot harmonisering van het materieel strafrecht en bevatten enkele bepalingen omtrent rechtshulp.[43] De bepalingen uit het Cybercrimeverdrag zijn voor de andere regionale cybercrimeverdragen zeker een inspiratiebron geweest. Bovendien hebben ze een belangrijke modelfunctie voor individuele landen die hun materiële en procedurele wetgeving op het gebied van computercriminaliteit willen aanpassen, ook zonder dat het desbetreffende land beoogt toe te treden tot het verdrag. Dit leidt tot een wereldwijde harmonisering, of in elk geval approximatie, van strafbepalingen omtrent delicten als computervredebreuk, kinderpornografie, denial-of-service-aanvallen en het bezit, de verspreiding en vervaardiging van kwaadaardige software. Ook de internationale uitwerking van het verdrag op het gebied van opsporingsbevoegdheden is belangrijk, omdat het verzekert dat staten digitaal bewijs kunnen verzamelen niet alleen om computercriminaliteit op hun eigen territorium op te sporen, maar ook op verzoek van andere staten. Daarbij kan wel de kanttekening worden geplaatst dat de implementatie van de materiële bepalingen van het verdrag systematischer en volledi ger lijkt te zijn dan de implementatie van de bepalingen betreffende opsporingsbevoegdheden.[44]
Hoewel het Cybercrimeverdrag, blijkens bovenstaande, een mondiale uitstraling heeft, zijn er inspanningen geweest om op het niveau van de Verenigde Naties tot een cybercrimeverdrag te komen. Een belangrijke reden daarvoor is dat het verdrag van de Raad van Europa, ondanks de mogelijkheid tot ratificatie door niet-Europese staten, gezien kan worden als een primair 'Westers' verdrag. De minder ontwikkelde landen waren niet bij de totstandkoming van het verdrag betrokken, waardoor de bepalingen in het verdrag mogelijk vooral georiënteerd zijn op de technisch ontwikkelde landen en mogelijk minder goed toepasbaar zijn voor de minder ontwikkelde landen.[45] De inspanningen om een VN-cybercrimeverdrag tot stand te brengen hebben echter (nog) niet tot succes geleid.[46] Hoewel het niet uitgesloten is dat een VN-verdrag alsnog tot stand komt, ligt het meer in de verwachting dat het Cybercrimeverdrag van de Raad van Europa de centrale rol zal (blijven) vervullen bij de internationale harmonisatie en samenwerking in digitale opsporing, gelet op de ruim zestig landen die dit verdrag inmiddels hebben geratificeerd en de nog steeds groeiende aansluiting van niet-Westerse landen bij dit verdrag.

42 Zie artikel 13 en 14 Richtlijn 2013/40/EU over aanvallen op informatiesystemen, *PubEU* L 218/8.
43 Zie UNODC 2013, p. 63-76 en Gercke 2014, p. 133-155 voor een overzicht van verdragen en initiatieven.
44 Franken 2015, p. 11.
45 Zie vooral Gercke 2014.
46 Zie in dit kader het rapport Chief Judge Stein Schjølberg, 'Report of the Chairman of HLEG to ITU Secretary-General Dr. Hamadoun I. Touré', *ITU Global Cybersecurity Agenda (GCA)*, High-Level Experts Group (HLEG) 2008, p. 6-9 en Gercke 2014, p. 129.

4.4 Grensoverschrijdende digitale opsporing

Het internationaal strafrecht is duidelijk: de uitvoerende jurisdictie van een staat is beperkt tot de territoriale grenzen van een staat. Dit beginsel staat op gespannen voet met de aard van internet dat niet tot de territoria van staten is beperkt. Internet faciliteert grensoverschrijdende opsporing en digitale rechercheurs willen daar graag gebruik van maken. Illustratief is daarvoor de volgende observatie van Koops & Goodwin in hun WODC-rapport over internationaal recht en grensoverschrijdende opsporing:

> *"In our research, we were struck by the lack of understanding with cyber-investigation experts of basic principles and developments of international law as well as by the lack of understanding with international law experts of basic principles and developments of cyber-investigation".*[47]

Staten blijven vooralsnog vasthouden aan het principe dat opsporing niet is toegestaan zonder toestemming van de betrokken staat of toestemming op basis van een verdrag.[48] Opsporing is een activiteit die aan de staat is voorbehouden. Het is onderdeel van de soevereiniteit van een staat om zelf te bepalen onder welke voorwaarden en door wie binnen zijn territorium opsporing mag plaatsvinden. Buitenlandse opsporingsinstanties die unilateraal en zonder toestemming of verdragsbasis opsporingshandelingen binnen het territorium van een andere staat uitvoeren, maken daarmee inbreuk op de soevereiniteit van de betrokken staat.[49]

Het internationaal strafrecht houdt met betrekking tot de kleine rechtshulp primair rekening met de soevereiniteit van de betrokken staten. De rechten en vrijheden van de betrokken burgers zijn daarbij van ondergeschikt belang. In Nederland komt dit bijvoorbeeld tot uiting in jurisprudentie, waarbij het uitgangspunt is dat de rechten en vrijheden van betrokken burgers niet direct worden geschaad bij unilaterale grensoverschrijdende opsporing.[50] Het idee is dat geen beschermd belang wordt overtreden en de opsporingshandelingen daarom niet tot een sanctie van een vormverzuim in de zin van artikel 359a Sv leiden. De Schutznorm is dus niet van toepassing als een opsporingshandeling de soevereiniteit van een andere staat schendt.

Toch moet helder zijn dat bij grensoverschrijdende opsporing ook de belangen van burgers worden geraakt. Als buitenlandse opsporingsautoriteiten onder hun eigen regels opsporingsmethoden toepassen die Nederlandse burgers of bedrijven raken, dan

47 Koops & Goodwin 2014, p. 78.

48 Zie Kaspersen 2007, p. 166: "Voor de beoordeling van de rechtmatigheid van die opsporingshandelingen in de virtuele wereld acht men de klassieke concepten als territoriale soevereiniteit nog steeds bepalend".

49 Zie ook paragraaf 4.2.2 en het Tallinn Manual 2017, p. 21.

50 HR 7 maart 2000, *NJ* 2000/539, m.nt. Sch. Zie meer recent Hof Den Haag, 27 april 2011, ECLI:NL:GHSGR:2011:BR6836, waarbij het hof oordeelt dat niet aan de Schutznorm (die stelt dat onrechtmatig verkregen bewijs in een strafproces wordt gesanctioneerd als de geschonden regel het belang van de verdachte beoogt te beschermen) wordt voldaan bij het hacken in een online account dat niet aan de verdachte toebehoort (maar waarbij wel gegevens zijn vergaard die van belang waren voor het opsporingsonderzoek).

is deze wetgeving voor Nederlandse burgers niet kenbaar en wordt hun rechtszekerheid aangetast, en – afhankelijk van de buitenlandse regeling – ook hun rechtsbescherming.[51] Het betreft een afgeleid beschermd belang, naast bescherming van de territoriale soevereiniteit van staten, dat de territoriale beperking van de uitvoerende jurisdictie beoogt te beschermen. Het systeem van rechtshulp moet aan de beperkingen die daaruit voortvloeien een oplossing bieden. Helaas blijkt uit onderzoek dat opsporingsautoriteiten ervaren dat het systeem van rechtshulp te traag is en onvoldoende de noodzaak van spoedeisende bewijsgaringsactiviteiten in cybercrimezaken adresseert.[52]

In deze paragraaf wordt daarom verkend in hoeverre unilaterale grensoverschrijdende opsporing tóch mogelijk is en, voor zover kenbaar uit publieke bronnen, welke praktijk reeds gaande is. Achtereenvolgens wordt de unilaterale toepassing van de volgende opsporingsmethoden besproken: (1) het grensoverschrijdend verzamelen van openbrongegevens, (2) grensoverschrijdende online undercover operaties, (3) de grensoverschrijdende netwerkzoeking, (4) het grensoverschrijdend vorderen van gegevens van online service providers en (5) de grensoverschrijdende toepassing van hacken als opsporingsmethode.

4.4.1 *Grensoverschrijdend verzamelen van gegevens uit open bronnen*

Artikel 32 sub a Cybercrimeverdrag biedt een grondslag voor het grensoverschrijdend vergaren van publiekelijk toegankelijke gegevens (open bronnen). Als de publiekelijk toegankelijke gegevens in andere staten opgeslagen zijn, dan zijn die ook toegankelijk voor de opsporingsautoriteiten van andere verdragspartijen. Artikel 32 sub a bepaalt dat daarvoor geen toestemming van de andere verdragspartij behoeft te worden verkregen. Toegang omvat tevens de bevoegdheid tot het maken van kopieën en het verdere gebruik van de gegevens.[53] De Cybercrimewerkgroep met betrekking tot "transborder access to computer systems" gaat zelfs zo ver dat de unilaterale grensoverschrijdende bewijsgaring op basis van publiekelijk toegankelijke gegevens als onderdeel van het internationaal gewoonterecht kan worden gezien.[54] In het Tallinn Manual 2.0 wordt hierbij aangesloten. Ook maken de experts duidelijk dat publiekelijk beschikbare gegevens op het *dark web* en gegevens die slechts toegankelijk zijn na registratie als "publiekelijke toegankelijke gegevens" moeten worden beschouwd.[55]
Een vraag die niet wordt geadresseerd in het Cybercrimeverdrag of in het Tallinn Manual 2.0 is of het op grond van deze bepaling ook mogelijk is stelselmatige observatie over de landsgrenzen heen toe te passen. Het waarnemen van gedragingen van perso-

51 Zie ook Oerlemans 2017a, p. 297.
52 Zie UNODC 2013, p. 214 en Koops & Goodwin 2014, p. 41.
53 Zie ook § 293 van de toelichting op het verdrag.
54 T-CY 2013, p. 10: "transborder access to publicly available data (Article 32(a)) may be considered accepted international practice and part of international customary law even beyond the Parties to the Budapest Convention".
55 Tallinn Manual 2017, p. 69-70.

nen in een online context kan ook als observatie worden aangemerkt (zie paragraaf 3.8.2). Stelselmatige observatie kan plaatsvinden door het stelselmatig (passief) volgen of waarnemen van gedrag van mensen op sociale media, zoals Twitter en Facebook. Het 'realtime' waarnemen van gedrag van de verdachte vangt aan vanaf het moment dat de observatie begint. Het onderscheidt zich daarmee van het stelselmatig verzamelen van gegevens omtrent personen uit open bronnen, waarbij historische gegevens worden verzameld. Voor de fysieke wereld heeft Nederland bijvoorbeeld in verdragen afgesproken onder welke omstandigheden observatie met een observatieteam grensoverschrijdend mag plaatsvinden. Het is een open vraag of artikel 32 sub a Cybercrimeverdrag kan worden geïnterpreteerd als een rechtsgrond voor unilaterale grensoverschrijdende stelselmatige observatie via internet. Ik ken geen zaken of nieuwsberichten waaruit blijkt dat staten tegen deze interpretatie protesteren.

4.4.2 *Grensoverschrijdende online undercover operaties*

In Nederland werd de praktijk van grensoverschrijdende online undercover operaties duidelijk in 2013. De Nederlander David Schrooten[56] was actief met online creditcardhandel. Bij de illegale handel in creditcards zijn al snel Amerikaanse hoofdrolspelers zoals MasterCard en Visa betrokken. De Amerikaanse Secret Service, belast met de opsporing van economische fraude in de Verenigde Staten, startte daarom een onderzoek naar de verdachte die op internet gebruik maakte van de alias 'Fortezza'. De opsporingsambtenaren maakten gebruik van een online account van een informant in een onderzoek naar de gestolen en verhandelde creditcardgegevens en legden op die manier onder dekmantel contact met 'Fortezza'. De Amerikaanse opsporingsambtenaren voerden een aantal gesprekken en een pseudokoop uit op de aangeboden creditcardgegevens. Na een vlucht naar Roemenië werd de verdachte aangehouden en op verzoek van de Verenigde Staten uitgeleverd. David Schrooten werd in de Verenigde Staten veroordeeld voor witwassen en creditcardfraude. Na contact van het Nederlandse ministerie van (toen nog) Veiligheid en Justitie met hun Amerikaanse collega's en een verzoek tot het uitzitten van de straf in Nederland, werd Schrooten een aantal weken na zijn aankomst in Nederland vrijgelaten.[57]
Bovenstaande zaak toont aan dat buitenlandse opsporingsinstanties in Nederland undercover opsporingsmethoden uitvoeren die in Nederland zijn gereguleerd als bijzondere opsporingsbevoegdheden, zoals pseudokoop en stelselmatige informatie-inwinning.[58] Als de Amerikanen weten dat een Nederlandse ingezetene in het opsporingsonderzoek betrokken is, moet volgens het internationale recht Nederland

56 De volledige naam wordt hier weergegeven, aangezien de betrokkene zelf met de gebeurtenissen in een boek naar buiten is getreden (David Schrooten & Freke Vuijst, *Alias Fortezza*, Balans 2016).

57 Zie Harry Lensink & Freke Vuijst, 'Geen krediet voor David S.', 16 maart 2013, *Vrij Nederland*. Beschikbaar op: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Geen-krediet-voor-David-S.-2.htm (laatst geraadpleegd op 1 juli 2018) en Harry Lensink, 'Minister wil terugkeer hacker David S. bespoedigen', 15 april 2013, Vrij Nederland. Beschikbaar op: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Minister-wil-terugkeer-hacker-David-S.-bespoedigen.htm (laatst geraadpleegd op 1 juli 2018).

58 Zie ook Oerlemans 2017a, p. 229-231.

om toestemming worden gevraagd om opsporingshandelingen op Nederlands territoir uit te voeren.[59] Het is de vraag of de Amerikaanse opsporingsambtenaren op de hoogte waren van de locatie van de verdachte. Het Nederlandse kabinet deelde in een Kamerbrief mee dat geen opsporingshandelingen op Nederlands grondgebied hebben plaatsgevonden, maar heeft zich uiteindelijk wel ingespannen David Schrooten weer naar Nederland te halen.[60]

In de media worden ook andere zaken genoemd met betrekking tot online drugsmarkten op het *dark web*, waarbij Amerikaanse opsporingsambtenaren pseudokopen in Nederland hebben uitgevoerd.[61] Ook hebben Australische rechercheurs in een spraakmakende zaak een kinderpornoforum op internet overgenomen en onder hun eigen (meer vergaande) wetgeving undercover operaties uitgevoerd met onmiskenbaar extraterritoriale gevolgen.[62] Ten slotte heeft de Nederlandse politie in een operatie in juli 2017 de online marktplaats 'Hansa' overgenomen en daarbij een maand lang alle drugsdeals en correspondentie van verdachten gevolgd.[63] Daarbij is het aannemelijk dat verschillende bijzondere opsporingsbevoegdheden onder Nederlands recht zijn ingezet, zoals infiltratie, stelselmatige informatie-inwinning en de telecommunicatietap. Het is ook helder dat daarbij (veel) buitenlandse verdachten betrokken zijn geweest.

Kortom, unilaterale online undercover operaties vinden regelmatig plaats, hoewel deze op gespannen voet staan met het verbod opsporingshandelingen in het buitenland te plegen zonder toestemming of verdragsbasis. Op internet is het echter niet altijd helder waar de betrokkene zich bevindt. Het (bijna uitsluitend) gebruik van nicknames op internet door cybercriminelen maakt het lastiger mensen op te sporen en te lokaliseren. Het kenmerkende aspect van het *dark web*, het feit dat de IP-adressen van computers in deze netwerken verborgen zijn, maakt het ook lastiger de betrokkenen en hun apparaten te lokaliseren. Met andere woorden, opsporingsinstanties kúnnen – zeker in het begin van een opsporingsonderzoek – niet altijd weten met wie zij te maken hebben en waar deze persoon of de computers waar zij gebruik van maken zich bevinden. Zij kunnen dan dus ook geen toestemming vragen aan een buitenlandse staat, omdat ze niet weten welke staat om toestemming moet worden gevraagd.[64]

De bovengenoemde voorbeelden laten ook zien dat de locatie van de computer waar de gegevens liggen opgeslagen en de locatie van de betrokkene de voornaamste 'lokalisatiemechanismen' zijn voor de opsporing.[65] Bevinden zich een van deze twee elementen

59 Zie ook Tallinn Manual 2017, p. 21.

60 Zie antwoord op Kamervragen over de uitlevering van een Nederlandse hacker David S. aan de Verenigde Staten door Roemenië van 7 juli 2012, *Aanhangsel Handelingen II* 2011/12, 3160 en antwoord op Kamervragen over het bericht 'FBI agenten hacken mee met Nederlandse politie' (...) van 15 april 2013, *Aanhangsel Handelingen II* 2012/13, 2001.

61 Zie Tom Kreling & Huib Modderkolk, 'De dealer die in de Amerikaanse val werd gelokt', *de Volkskrant*, 7 juni 2016.

62 NOS Nieuws, 'Australische politie nam enorme kinderpornowebsite over', 8 oktober 2017.

63 Huib Modderkolk, 'Zo nam de Nederlandse politie een online drugsmarkt over', 19 augustus 2017, *De Volkskrant*.

64 Zie ook Oerlemans 2017a, p. 338.

65 Zie ook Oerlemans & Conings 2013 over het 'computergeoriënteerd juridisdictiebeginsel' en Conings 2014 over de lokalisatie van personen en objecten in deze context.

in het buitenland, dan zullen opsporingsinstanties te rade moeten gaan hoe ver zij mogen gaan in hun opsporingshandelingen. In de situatie dat het onduidelijk is waar de verdachte zich bevindt en niet rederlijkwijs is vast te stellen waar de verdachte zich bevindt, bijvoorbeeld omdat de verdachte onder een nickname actief is op het *dark web*, ben ik van mening dat opsporingsinstanties tot een unilaterale toepassing van de bevoegdheden mogen overgaan.[66]

In onder andere het Tallinn Manual 2.0 wordt bevestigd dat staten zich niet mogen bemoeien met de taak van andere staten door via internet opsporingshandelingen te verrichten waar buitenlandse ingezetenen bij betrokken zijn. Maar als de lokalisatie van de verdachten niet rederlijkwijs is vast te stellen, bestaat hier mogelijk wel ruimte voor. Opgemerkt zij ook dat niet alle staten hetzelfde denken over de toelaatbare grenzen van de opsporingshandelingen met extraterritoriale gevolgen. De Verenigde Staten heeft regelmatig undercover operaties op buitenlands grondgebied uitgevoerd. Mogelijk worden deze opsporingshandelingen aldaar niet als problematisch ervaren, omdat zij in de Verenigde Staten niet als opsporingshandelingen worden gezien die een inmenging op de rechten en vrijheden van personen met zich meebrengen. Ook speelt mogelijk de politieke machtsverhouding tussen staten een rol en daarmee de bereidheid van sommige staten verder te gaan met extraterritoriale opsporing dan andere staten.[67]

Het Cybercrimeverdrag rept met geen woord over undercover operaties op internet en regulering van deze opsporingsmethoden. Om dezelfde reden wordt daarom in het verdrag ook geen aandacht besteed aan de eventuele unilaterale toepassing daarvan. Het hoofd van Europol heeft in het kader van een cybercrime-rapport wel opgeroepen tot regelgeving voor online undercover operaties op het *dark web*.[68] Deze oproep heeft echter vooralsnog geen gevolg gekregen in Europese wet- en regelgeving. Het ontbreekt om deze reden vooralsnog aan duidelijkheid in hoeverre deze vorm van unilaterale opsporing in online omgevingen internationaalrechtelijk gezien toelaatbaar is.

4.4.3 *Grensoverschrijdende netwerkzoeking*

In de toelichting van de Wet computercriminaliteit II heeft de Nederlandse wetgever duidelijk gemaakt dat tijdens een netwerkzoeking geen toegang mag worden verschaft tot een computer die zich op buitenlands territorium bevindt.[69] Dit verbod is terug te voeren op het idee dat de extraterritoriale effecten van een netwerkzoeking zijn gebaseerd op de locatie van de opgeslagen gegevens op een computer (het computergeoriënteerd jurisdictiebeginsel). Het toegang verschaffen zonder toestemming of verdragsbasis met de betrokken staat wordt in dat geval gezien als een inbreuk op de

66 Zie ook Oerlemans 2017a, p. 338.
67 Zie ook Nadelmann 1993 en Oerlemans 2017a, p. 328.
68 Europol, IOCTA-rapport 2016, 14: "The difficulties faced by law enforcement operating lawfully in the Darknet are clear, with many jurisdictions restricted by national legislation. A harmonised approach to undercover investigations is required across the EU".
69 Zie *Kamerstukken II* 2004/05, 26671, 10, p. 13.

territoriale soevereiniteit van die staat.[70] Deze interpretatie is ook terug te vinden in artikel 19 lid 2 van het Cybercrimeverdrag over de netwerkzoeking, waar wordt gesproken over de data die staan opgeslagen in een (deel van het) computersysteem "in its territory".

De territoriale beperking van de netwerkzoeking brengt aanzienlijke praktische problemen met zich mee. Steeds vaker staan gegevens op computers elders opgeslagen, vanwege het toenemende gebruik van cloud computing. Daarbij kan bijvoorbeeld worden gedacht aan het gebruik van het programma Office 365 van Microsoft, waarbij gegevens standaard worden opgeslagen op servers in het beheer van Microsoft die zich overal ter wereld in datacentra bevinden. Spoenle wees er als een van de eersten op dat door cloud computing de locatie van gegevens op computers niet meer redelijkerwijs kan worden vastgesteld.[71] Cloud computing maakt het mogelijk dat gegevens constant tussen servers bewegen die mogelijk in verschillende datacentra op de wereld verspreid staan. Gecombineerd met het feit dat ook de locatie van servers niet altijd goed is vast te stellen, betekent dit dat de locatie van gegevens moeilijk bepaalbaar is. Koops & Goodwin noemen dit het "loss of knowledge of location"-probleem.[72] Dit duidt aan dat gegevens weliswaar nog steeds een locatie hebben (en er dus niet, zoals Spoenle stelt,[73] een "loss of location"-probleem is), maar dat de kenbaarheid van de locatie het probleem is. De vraag in dat licht is op welke manier het strikte uitgangspunt van de territoriale beperking bij de toepassing van opsporingsbevoegdheden ten uitvoer kan of moet worden gelegd. Het internationale recht geeft hier vooralsnog geen duidelijkheid over.[74]

In het kader van de Wet computercriminaliteit II merkt de Nederlandse wetgever hierover op dat wanneer opsporingsambtenaren de locatie van de data niet meer redelijkerwijs kunnen vaststellen, een mogelijke grensoverschrijdende netwerkzoeking is toegestaan.[75] De toelichting in de conceptwetsvoorstellen in het kader van het project 'modernisering strafvordering' gaat een stuk verder. Hier wordt aangegeven dat een netwerkzoeking zonder meer kan strekken tot een doorzoeking van een webmailaccount (zoals Gmail) of een online opslagdienst (zoals Dropbox).[76] Samen met Conings ben ik van mening dat een grensoverschrijdende netwerkzoeking is toegestaan, indien de verdachte (rechts)persoon zich bevindt in het territorium van de onderzoekende staat en de opsporende instanties rechtmatig de vereiste inloggegevens hebben verkregen.[77] Koops en Goodwin geven ook aan dat de inbreuk op de territoriale soevereiniteit bij een dergelijke grensoverschrijdende netwerkzoeking zeer beperkt blijft.[78] Niettemin

70 Zie ook Koops & Goodwin 2014, p. 61.
71 Spoenle 2010, p. 4-5.
72 Koops & Goodwin 2014, p. 48.
73 Spoenle 2010.
74 Zie ook Tallinn Manual 2017, p. 68.
75 *Kamerstukken II* 2004/05, 26671, 10, p. 23.
76 Zie het discussiestuk 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken' van 6 juni 2014, p. 52-53.
77 Conings & Oerlemans 2013, p. 29-30. Zie ook Oerlemans 2017a, p. 340.
78 Koops & Goodwin 2014, p. 76. Zie ook Conings 2014, p. 14.

bestaat er geen expliciete verdragsbasis voor dergelijk handelen.[79] Als achteraf blijkt in welke staat de gegevens lagen opgeslagen, ligt het in de rede – vergelijkbaar met de bepaling over grensoverschrijdend tappen – de buitenlandse staat in te lichten en om toestemming te vragen alvorens de gegevens als bewijs te gebruiken (zie ook paragraaf 3.2.4).

4.4.4 *Grensoverschrijdend vorderen van gegevens*

In paragraaf 4.4.3 is al opgemerkt dat steeds meer gegevens liggen opgeslagen bij online dienstverleners die van cloud computing-diensten gebruikmaken. Deze tendens is ook van belang bij het vorderen van gegevens die voor een opsporingsonderzoek van belang zijn. Daarbij kan gedacht worden aan het vorderen van gebruikersgegevens, verkeersgegevens, loggegevens en opgeslagen inhoudsgegevens.
Artikel 32 sub b Cybercrimeverdrag voorziet in een verdragsbasis om gegevens te verkrijgen van een bedrijf of persoon, waarbij de betrokkene die rechtmatig over de gegevens kan beschikken, *vrijwillig* gegevens verstrekt.[80] Artikel 32 sub b Cybercrimeverdrag voorziet dus niet in een verdragsbasis om unilateraal gegevens te *vorderen* van buitenlandse providers. Gercke omschrijft artikel 32 sub b Cybercrimeverdrag als een vreemde in de bijt, omdat hierbij *bedrijven* de bevoegdheid krijgen vrijwillig gegevens te verstrekken aan buitenlandse autoriteiten, terwijl normaliter *staten* beslissen of zij opsporingshandelingen binnen hun territorium toestaan.[81] De bepaling wordt door sommige staten, zoals Rusland, gezien als een onacceptabele inbreuk op hun soevereiniteit en als reden aangedragen het Cybercrimeverdrag niet te ondertekenen.[82] Een moeilijkheid bij deze regeling is dat dienstaanbieders alleen gegevens kunnen verstrekken als zij dat rechtmatig kunnen doen, terwijl de vrijwillige verstrekking van gegevens veelal beperkt is in verband met gegevensbeschermingsregels[83] of het feit dat staten toepassing van hun eigen nationale regelgeving voorschrijven bij de verstrekking van gegevens van opsporingsdiensten.[84]
De Cybercrime Convention Committee (T-CY) van de Raad van Europa benadrukt in een rapport dat verdragsstaten de bevoegdheid om gebruikersgegevens te vorderen, kunnen toepassen op dienstverleners die hun diensten aanbieden binnen het territori-

79 In het Tallinn Manual 2.0 (2017, p. 15-16) wordt aangegeven dat slechts een minderheid van de experts de interpretatie volgt dat in deze situatie een grensoverschrijdende netwerkzoeking is toegestaan.
80 Artikel 32 sub b Cybercrimeverdrag luidt als volgt: "A Party may, without the authorisation of another Party: (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system".
81 Gercke 2012, p. 277.
82 Zie Koops e.a. 2012b, p. 37 en Tallinn Manual 2017, p. 70.
83 Zie in dit verband ook T-CY 2014, p. 14, waarin de werkgroep duidelijk maakt dat een bepaling in de algemene voorwaarden van dienstaanbieders niet voldoet als een vorm van toestemming van de betrokkene voor een vrijwillige verstrekking van gegevens aan opsporingsinstanties.
84 Zie de 'Article 29 Working Party's comments on the issue by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime', brief aan de Raad van Europa van 5 december 2013, p. 3. Zie ook Koops & Goodwin 2014, p. 45.

um van de verdragsstaat, maar daar niet juridisch of fysiek aanwezig zijn.[85] Een dienstverlener kan bijvoorbeeld zijn hoofdkwartier in de ene staat hebben, terwijl de gegevens liggen opgeslagen op het territorium van een andere staat. Opgemerkt wordt dat de locatie van gegevens steeds vaker niet meer de bepalende factor is om jurisdictie te bewerkstelligen. Tegelijkertijd wordt daarbij gezegd dat deze '*guidance note*' op zichzelf geen toestemming inhoudt voor het extraterritoriaal vorderen van gegevens bij dienstverleners op buitenlands grondgebied en geen nieuwe verplichtingen voor verdragsstaten oplevert. De opstellers van het verdrag lieten destijds in het midden of een dergelijke unilaterale vordering in strijd is met het internationaal recht.[86]
De expertgroepen met betrekking tot 'transborder access' (dat wil zeggen unilaterale grensoverschrijdende toegang tot gegevens) van het Cybercrimeverdrag onderzoeken al jaren of er afspraken gemaakt kunnen worden onder welke voorwaarden unilaterale toegang mogelijk is. Deze inspanningen beogen te resulteren in een Tweede Protocol bij het Cybercrimeverdrag; hierop wordt in paragraaf 4.5 verder ingegaan.
In dit kader is het opmerkelijk te noemen dat in België een praktijk groeit waarbij Belgische autoriteiten Amerikaanse dienstverleners verplichten direct, onder Belgisch recht, gegevens na een vordering te verstrekken. Het Belgische Hof van Cassatie heeft Yahoo! Inc veroordeeld voor het niet-voldoen aan een vordering tot verstrekking van gebruikersgegevens.[87] Ook Skype, nu onderdeel van Microsoft, is in België veroordeeld voor het niet-meewerken aan het faciliteren van een telecommunicatietap onder Belgisch recht.[88] Verschillende auteurs zijn van mening dat Hof van Cassatie ten onrechte de territoriale beperking van de uitvoerende jurisdictie negeert en in strijd met het internationale recht handelt.[89] Het is ook praktisch de vraag hoe een dergelijke boete ten uitvoer wordt gelegd, als er geen aanspreekbare (rechts)personen of in beslag te nemen objecten op Belgisch grondgebied te vinden zijn.

In de tussentijd heeft zich een praktijk ontwikkeld waarbij opsporingsdiensten overal ter wereld direct gebruikersgegevens en verkeersgegevens kunnen vorderen bij grote Amerikaanse dienstverleners zoals Microsoft, Google en Facebook.[90] Deze dienstverleners bepalen vervolgens zelf, via advocaten of hun *legal compliance*-afdeling, of zij *op vrijwillige basis* aan deze vordering gehoor geven.[91] Voor het verkrijgen van opgeslagen e-mails of documenten bij deze providers is overigens vooralsnog een toestemming (een 'warrant') van een Amerikaanse rechter noodzakelijk, wat betekent dat de weg van wederzijdse rechtshulp moet worden bewandeld. Inmiddels heeft de VS echter de

85 Zie T-CY 2017, p. 6.
86 Zie ook paragraaf 291 van de toelichting op het verdrag.
87 Zie over deze zaak uitgebreid De Schepper & Verbruggen 2013 en Verbruggen 2014.
88 Rb. van eerste aanleg Antwerpen 27-10-2016, ECLI:NL:XX:2016:183, *Computerrecht* 2017/6, m.nt. E. Valgaeren.
89 Zie De Schepper & Verbruggen 2013, p. 164 en Verbruggen 2014, p. 137. Zie anders: Kerkhofs & Van Linthout 2013.
90 Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 9.
91 Zie, bijvoorbeeld, het beleid zoals omschreven in de jaarlijkse transparantierapporten van Google en Microsoft.

'Clarifying Overseas Use of Data Act' (CLOUD Act) aangenomen, die mogelijk flinke veranderingen met zich meebrengt, omdat deze wet het mogelijk maakt overeenkomsten af te sluiten met andere landen om wel – onder bepaalde voorwaarden – rechtstreeks gegevens bij buitenlandse aanbieders te vorderen (zie verder paragraaf 4.5.1).

4.4.5 *Grensoverschrijdend hacken*

De hackbevoegdheid (vergelijk paragraaf 3.7) kan eenvoudig over de territoriale grenzen van staten worden toegepast. Internet kent geen territoriale grenzen en hierdoor kunnen opsporingsambtenaren technisch gezien op afstand computers op buitenlands territoir binnendringen. Zoals meermaals in dit hoofdstuk is uitgelegd, is het echter niet toegestaan zonder toestemming van een staat of verdragsbasis opsporingshandelingen in het buitenland te plegen. Dat geldt uiteraard ook voor hacken. Deze hoofdregel wordt in de wetsgeschiedenis van de Wet computercriminaliteit III bevestigd.[92]
Tegelijkertijd zijn er situaties denkbaar waarbij tijdens de bewijsverzameling in een opsporingsonderzoek de locatie van (gegevens op) computers niet helder is. Het is, met andere woorden, redelijkerwijs niet meer mogelijk deze locatie altijd vast te stellen. Dat kan bijvoorbeeld het geval zijn, indien verdachten in een opsporingsonderzoek gebruikmaken van het Tor-netwerk.[93] In de memorie van toelichting bij de Wet computercriminaliteit III wordt aangegeven dat het in bepaalde omstandigheden voor opsporingsambtenaren mogelijk is hacken als opsporingsbevoegdheid over territoriale grenzen toe te passen. Meer specifiek wordt aangegeven dat dit mogelijk moet zijn als de verdachte gebruikmaakt van cloud computing-technieken en anonimiseringsdiensten.[94] De locatie van de computers waarop toegang wordt verschaft, is in die gevallen namelijk niet meer redelijkerwijs vast te stellen.[95] Als daarvan sprake is moet dat expliciet in het bevel van de officier van justitie tot toepassing van deze bijzondere opsporingsbevoegdheid worden vermeld. Als tijdens het onderzoek de locatie van de gegevens alsnog duidelijk wordt, moet alsnog een rechtshulpverzoek naar de betrokken staat worden gestuurd, waarbij aan de bevoegde buitenlandse autoriteiten verantwoording wordt afgelegd over de handelingen die tot dan toe zijn verricht en de afwegingen die daarbij zijn gemaakt. Als achteraf duidelijk wordt dat de gegevens zich op het territorium van een andere staat bevonden, dan moet op de kortst mogelijke termijn alsnog toestemming worden gevraagd aan het desbetreffende land.[96]
Het valt te bezien hoe in de praktijk met deze verplichtingen wordt omgegaan, omdat het bewijs in die gevallen dan al effectief is vergaard en het halverwege of achteraf toestemming vragen aan een andere staat de nodige tijd kan vergen. De andere staat zal

92 *Kamerstukken II* 2015/16, 34372, 3, p. 44 en *Kamerstukken II* 2016/17, 34372, 6, p. 56 en 96.
93 Zie paragraaf 3.7.1 over het Tor-netwerk en het anonimiteitsprobleem. Zie ook uitgebreid Oerlemans 2017a, p. 338-342.
94 Interessant is dat in de Verenigde Staten 'Rule 41' van de Federal Rules of Criminal Procedure wordt aangepast, waarbij onder vergelijkbare voorwaarden op afstand toegang kan worden verschaft tot computers die mogelijk in het buitenland staan. Zie verder Oerlemans 2017b.
95 *Kamerstukken II* 2015/16, 34372, 3, p. 47-48 en *Kamerstukken II* 2016/17, 34372, 6, p. 96.
96 *Kamerstukken II* 2015/16, 34372, 3, p. 47 en *Kamerstukken II* 2016/17, 34372, 6, p. 96.

vaak geen belang hebben het verzoek met voorrang te behandelen, omdat er immers geen risico meer is op verlies van gegevens. Ook bestaat het risico dat de staat achteraf toestemming weigert en de gegevens dan niet als bewijs kunnen worden gebruikt. Mogelijk bestaat er ook geen behoefte om achteraf toestemming te vragen, als bijvoorbeeld blijkt dat er onvoldoende aanknopingspunten zijn voor vervolging en gegevens dus niet als bewijs hoeven te worden gebruikt. Om uiteenlopende redenen is er dus geen duidelijke prikkel voor de Nederlandse opsporingsautoriteiten om buitenlandse staten achteraf om toestemming te vragen, zeker als zij zich kunnen verschuilen achter het argument dat de locatie van de gegevens niet met voldoende zekerheid kon worden achterhaald. De belangrijkste prikkel om dat wel te doen is vermoedelijk het risico van internationaal of diplomatiek protest van de staat op wiens grondgebied, zonder zijn toestemming, gegevens via hacken zijn vergaard. Dat risico is niet erg groot, maar ook niet verwaarloosbaar. Aan de ene kant is het lastig voor een staat om heimelijk opsporingshandelingen van andere staten op zijn eigen territorium op te merken. Aan de andere kant kunnen feiten over de unilaterale hack – naar aanleiding van een rechtszaak en de media-aandacht die sommige zaken krijgen – naar buiten komen, hetgeen tot protest kan leiden in de betrokken staat.[97]

De wenselijkheid van deze (mogelijk extraterritoriale) toepassing van hacken als opsporingsbevoegdheid moet volgens de toelichting op de Wet computercriminaliteit III worden afgewogen aan de hand van verschillende criteria. Deze criteria hebben betrekking hebben op:

1. de inspanning die is vereist om de identiteit en locatie van een geautomatiseerd werk te achterhalen;
2. de ernst van het strafbare feit;
3. de mate van betrokkenheid van de Nederlandse rechtsorde (betrokkenheid van Nederlandse slachtoffers of de Nederlandse infrastructuur);
4. de aard van de te verrichten opsporingshandelingen (worden gegevens alleen overgenomen of ook ontoegankelijk gemaakt?); en
5. de risico's voor het geautomatiseerde werk.[98]

Koops & Goodwin hebben hierover terecht opgemerkt dat in de toelichting ten onrechte het belang van het reciprociteitsprincipe niet wordt genoemd.[99] Staten kunnen namelijk met een beroep op dat principe onder vergelijkbare gevallen zich ook in Nederland op afstand toegang verschaffen tot geautomatiseerde werken. Die wens van andere staten is niet denkbeeldig, gezien de omvangrijke hostingindustrie in Nederland. Ook kan kritiek worden geleverd op het feit dat een officier van justitie en rechter-commissaris de keuze moeten maken de bevoegdheid grensoverschrijdend toe te passen. Ligt het niet meer voor de hand een apart, statelijk orgaan deze keuze te laten

97 John Leyden, 'Russians accuse FBI agent of hacking', *The Register*, 16 augustus 2002. Beschikbaar op: http://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/ (laatst geraadpleegd op 1 juli 2018).
98 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 48.
99 Koops & Goodwin 2014, p. 86.

maken in plaats van opsporingsautoriteiten, gezien de mogelijke politieke gevolgen van de grensoverschrijdende toepassing van indringende opsporingsmethoden? Aan de andere kant is er ook sympathie voor de werkwijze, omdat met bepaalde belangen rekening wordt gehouden en het de mogelijkheid biedt voor de politie en het Openbaar Ministerie effectiever op te treden tegen cybercrime. Als geen enkele mogelijkheid wordt gegeven potentieel over de territoriale grenzen van staten te treden, zal de politie in veel situaties met lege handen komen te staan en leidt dat volgens de regering tot 'vrijplaatsen op internet'.[100] Koops & Goodwin vatten het perspectief van de Nederlandse wetgever mooi samen door op te merken dat Nederland op deze wijze een vergaande grensoverschrijdende toepassing van de hackbevoegdheid mogelijk maakt, die sterk leunt op een pragmatische insteek en minder op een strikte interpretatie van de wet.[101]

4.5 Naar een toekomstige regeling van grensoverschrijdende digitale opsporing

Uit paragraaf 4.4 moet duidelijk zijn geworden dat er veel discussie bestaat over de territoriale reikwijdte van opsporingsbevoegdheden die toepassing vinden op internet. De discussie binnen internationale gremia richt zich vooralsnog voornamelijk op het vorderen van gegevens, omdat dit het meest urgente en meest zichtbare knelpunt lijkt te zijn. In deze paragraaf behandel ik de belangrijkste internationale initiatieven die bepalend lijken voor de toekomstige regeling van de grensoverschrijdende digitale opsporing.

4.5.1 *U.S. Cloud Act*

De 'Clarifying Overseas Use of Data Act' (CLOUD Act) van 23 maart 2018[102] maakt het mogelijk dat niet-Amerikaanse opsporingsautoriteiten toegang kunnen krijgen tot gegevens van Amerikaanse dienstverleners als aan bepaalde voorwaarden wordt voldaan. Deze afspraken moeten worden gemaakt in een zogenoemd 'executive agreement'. Als een 'executive agreement' van kracht is, kunnen niet-Amerikaanse opsporingsdiensten gegevens vorderen van Amerikaanse dienstverleners onder hun eigen regelgeving, voor zover de gegevens geen betrekking hebben op Amerikaanse burgers. De vordering moet verder betrekking hebben op ernstige criminaliteit, door een onafhankelijke autoriteit (kunnen) worden getoetst, voldoende specifiek zijn en voldoen aan de nationale regelgeving van de desbetreffende staat.[103] Als onderdeel van het principe van

100 *Kamerstukken II* 2015/16, 34372, 3, p. 51
101 Zie Koops & Goodwin 2014, p. 86. Ook Zoetekouw 2017 is kritisch over de wetsinterpretatie in de toelichting en stelt dat het "geen basis in het internationaal recht" heeft.
102 CLOUD-Act: H.R.1625 – 115th Congress, 866 et seq, onderdeel van de 'Consolidated Appropriations Act, 2018'. Deze wet past de Amerikaanse 'Stored Communication Act' aan.
103 Zie C. Conings, 'The CLOUD-Act: U.S. sets the rules for cross-border e-evidence gathering?', 11 april 2018, Stibbe blog.

reciprociteit krijgen ook Amerikaanse dienstverleners de mogelijkheid tot directe toegang tot de gegevens van internetdienstverleners op het grondgebied van andere desbetreffende staten. Amerikaanse dienstverleners krijgen de mogelijkheid protest aan te tekenen als zij denken dat de verstrekking van gegevens van een niet-Amerikaan of persoon die zich buiten de VS bevindt in strijd is met de regelgeving van een ander land. Een Amerikaanse rechtbank besluit dan op basis van 'balanceertest' of de gegevens moeten worden afgegeven. Nederland heeft op het moment van schrijven (medio juli 2018) nog geen 'executive agreement' afgesloten met de Verenigde Staten.

4.5.2 *Een Tweede Protocol bij het Cybercrimeverdrag*

Sinds de totstandkoming van het Cybercrimeverdrag in 2001 staat de verdere ontwikkeling van het verdrag niet stil. Er zijn inmiddels tientallen rapporten verschenen van werkgroepen met experts die uitleg bieden omtrent bepalingen van het Verdrag. Ook wordt gewerkt aan aanvullende bepalingen voor het verdrag, waarbij vooral veel aandacht uitgaat naar de in dit hoofdstuk behandelde problematiek door middel van werkgroepen betreffende 'transborder access to data' (2012-2014) en 'cloud evidence' (2015-2017). Het is daarbij niet eenvoudig gebleken resultaten te boeken, omdat elke staat vanuit zijn eigen achtergrond en cultuur vaak anders denkt over strafbaarstellingen, bevoegdheden en de territoriale beperkingen bij de toepassing van opsporingsmethoden. In de loop der jaren is wel duidelijk geworden dat het gebrek aan afdwingbare mogelijkheden om unilateraal gegevens te verzamelen bij buitenlandse internet service providers het effectief verzamelen van bewijsmateriaal in cybercrime-onderzoeken in de weg staat, zodat de noodzaak van een internationale aanpak van deze problematiek steeds hoger op de agenda is gekomen. De werkgroepen van de Raad van Europa hebben daarom aanzienlijke inspanningen geleverd om tot aanvullende bepalingen van het Cybercrimeverdrag te komen om het unilateraal verkrijgen van toegang tot gegevens mogelijk te maken.
Deze inspanningen hebben geleid tot de voorbereiding van een Tweede Protocol bij het Cybercrimeverdrag in 2017.[104] De tekst en toelichting van het Tweede Protocol moeten volgens de planning in december 2019 voltooid zijn. De belangrijkste bepalingen uit de 'terms of reference' van het protocol betreffen de verbetering van wederzijdse rechtshulp, directe samenwerking met aanbieders in andere staten, een raamwerk en waarborgen voor bestaande praktijken van grensoverschrijdende toegang tot data, en rechtsstatelijke en gegevensbeschermingsrechtelijke waarborgen.[105] Op die wijze moet het direct (unilateraal) vorderen van gegevens bij online dienstverleners in het buiten-

104 Zie het persbericht op de bijeenkomst van de T-CY werkgroep van 7 tot 9 juni 2017 en de goedgekeurde 'terms of reference' van het Tweede Protocol op 8 juni 2017.

105 Zie de samenvatting op https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713 (laatst geraadpleegd 1 juli 2018). Zie uitgebreider Cybercrime Convention Committee (T-CY), Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, T-CY (2017)3, 9 juni 2017, https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b (laatst geraadpleegd 1 juli 2018).

land mogelijk worden en moet de bestaande, ondergenormeerde praktijk van unilaterale grensoverschrijdende opsporing beter worden ingekaderd.
De werkgroep beoogt aldus ook het regime voor het vorderen van gegevens via rechtshulp te vereenvoudigen, met behulp van direct contact tussen opsporingsautoriteiten, het voorschrijven van de vorderingen in de Engelse taal en het creëren van spoedaanvragen voor het vorderen van gegevens. Daarbij houdt de werkgroep het belang voor ogen van voldoende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder het recht op gegevensbescherming.[106]

4.5.3 *EU-voorstellen*

Ook binnen de Europese Unie worden inspanningen geleverd om eenvoudiger toegang te krijgen tot gegevens bij internetdienstverleners. Op 17 april 2018 heeft de Europese Commissie twee voorstellen in consultatie gegeven over het verkrijgen van gegevens van internetdienstverleners in strafzaken.[107] De nieuwe regelgeving moet opsporingsinstanties de instrumenten geven direct vorderingen te sturen naar internetdienstverleners. De conceptrichtlijn verplicht EU-lidstaten om wetgeving te maken die internetdienstverleners verplicht stelt een vertegenwoordiger aan te stellen om deze vordering in ontvangst te nemen. Aan de vordering moet binnen tien dagen, en in noodgevallen binnen zes uur, worden voldaan. Internetdienstverleners kunnen zich tegen de vordering verzetten als daar een grondslag voor is in hun eigen wetgeving of in wetgeving in een derde land. Ook staat de mogelijkheid van verzet open als de vordering onmiskenbaar in strijd is met het Handvest van de Grondrechten van de Europese Unie.
De voorgestelde regeling bevat enkele waarborgen ter bescherming van de persoonlijke levenssfeer. Het vorderen van verkeersgegevens en inhoudelijke gegevens moet gevalideerd worden door een rechter. Ook is de vordering beperkt tot bepaalde categorieën van misdrijven, zoals de meer ernstige misdrijven, waarvoor een gevangenisstraf van drie jaar of meer is voorgeschreven en specifieke cyber- en terroristische misdrijven.
De regeling is van toepassing op internetdienstverleners die één of meer ondernemingen binnen de EU hebben of als een 'substantiële connectie met de Europese Unie' bestaat, bijvoorbeeld vanwege substantieel veel klanten in lidstaten of als de dienstverlener zijn activiteiten specifiek richt op bewoners van EU-lidstaten. De regeling wordt noodzakelijk geacht omdat internetdienstverleners te maken hebben met een gefragmenteerd stelsel van regelingen voor het vorderen van gegevens door opsporingsautoriteiten van de verschillende EU-lidstaten. Ook kost het vergaren van deze vorm van

106 *Ibid.*
107 Voorstel van 17 april 2018 voor een Verordening betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken, COM(2018) 225 en Voorstel van 17 april 2018 voor een Richtlijn tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures, COM(2018) 226. Zie ook J.J. Oerlemans, *T&C Internationaal strafrecht*, Cybercrimeverdrag, aant. 7.

digitaal bewijs van internetdienstverleners volgens de Commissie onder het huidige stelsel (te) veel tijd.
Het is nog niet duidelijk of deze wetgeving doorgang vindt en hoe de definitieve versie eruit komt te zien.

4.5.4 *Afsluiting*

De Amerikaanse Cloud Act en de EU-voorstellen zijn de meest kansrijke initiatieven om te komen tot een multinationale regeling van grensoverschrijdende opsporing. Het wachten is op concrete overeenkomsten die de VS onder de Cloud Act zullen afsluiten met individuele landen, en op de verdere ontwikkeling van de EU-voorstellen. Beide initiatieven zijn beperkt tot het rechtstreeks benaderen van buitenlandse internetdienstverleners om gegevens te verkrijgen.
Uit paragraaf 4.4 blijkt echter dat dezelfde problematiek van uitvoerende rechtsmacht speelt bij de toepassing van andere opsporingsbevoegdheden, zoals online undercover opsporingsmethoden en hacken als opsporingsbevoegdheid. Het is dan ook wenselijk dat de internationale discussie en initiatieven zich verbreden tot grensoverschrijdende digitale opsporing in meer algemene zin.
De ontwikkeling van een Tweede Protocol bij het Cybercrimeverdrag kan daar een welkome bijdrage aan leveren, omdat het niet alleen beoogt rechtshulpprocedures te versoepelen en directe benadering van service providers te faciliteren, maar ook kaders zou moeten bieden voor 'bestaande praktijken' van grensoverschrijdende opsporing. Die in potentie bredere aanpak heeft als voordeel dat het een meer omvattende regeling kan bewerkstelligen dan de initiatieven in de VS en de EU. Tegelijkertijd vormt die bredere aanpak ook een nadeel, omdat het de onderhandelingen complexer maakt. Daarnaast blijft het de vraag hoeveel landen een protocol met een bredere regeling zouden ratificeren. Vermoedelijk zal een voorzichtige, stapsgewijze aanpak het meest haalbaar zijn.
Het is soms lastig te accepteren dat deze discussies in internationale gremia zo langzaam en lastig verlopen. De digitalisering van criminaliteit én de opsporing dendert ondertussen voort. Staten zullen zich genoodzaakt voelen te handhaven en in bepaalde gevallen unilateraal grensoverschrijdend te werk te gaan. Daarbij kunnen de rechten en vrijheden van de betrokkenen in het gedrang komen. Het onderwerp van grensoverschrijdende digitale opsporing ligt echter – zoals aangegeven – vooral gevoelig omdat het direct betrekking heeft op de soevereiniteit van staten. Daarnaast spelen in onderhandelingen en het opstellen van verdragen natuurlijk ook de relaties tussen staten en politieke gevoeligheden een rol. Dit stemt helaas niet optimistisch over de resultaten die op het brede spectrum van digitale grensoverschrijdende opsporing in de komende vijf jaar kunnen worden behaald. Opsporingsinstanties, waaronder de Nederlandse autoriteiten, zullen dus in de tussentijd bewust om moeten gaan met grensoverschrijdende digitale opsporing en een eigen beleid moeten ontwikkelen.